
Governance, Legislation and Ethics Work-Based Project

ACCA5016

Adam Vimpany

1810613

Submitted 11th September 2020

Report FAO: The Head of Information Governance

Summary

The purpose of this report is to outline an incident that resulted in a breach of confidential data from within the operational department.

Personal identifiable data (PII), as defined under the GDPR¹, has leaked to a member of the public. The leaked data includes the names and addresses of staff members and is held for valid reasons (staff administration). The data is securely stored within an operational system; however, it is possible for members of staff with the correct privileges (in this case the operational manager) to access and download the data onto local devices. In the event of this particular breach, the manager extracted the data with the objective of “working more efficiently”.

The breach occurred when the list of PII (as defined by the ICO under the GDPR)² was inadvertently e-mailed to a single member of the public. Although the incident is isolated to the one subject, it is imperative to properly investigate and assess the risk as the incident is in clear breach of the Data Protection Act 2018³. Further investigation did not identify any further breaches; however, there is cause for concern as scanned sick notes and occupational health reports were found on the manager’s desktop.

Data protection implications

The data breach contained personal data as defined by the GDPR⁴. There was no special category data leaked, although a serious risk was identified during the investigation: both sick notes and occupational health reports contain special category data⁵ and were found on the manager’s desktop. This has been scrutinised as part of the risk assessment and will be a prime consideration for the recommendations set out by the report. This is significant as the implications for leaked special category data carry a higher severity and are much more likely to result in bad press or induce regulatory fines.

¹ "General Data Protection Regulation (GDPR)." <https://gdpr-info.eu/>. Accessed 10 Sep. 2020.

² "What is personal data? | ICO." <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>. Accessed 10 Sep. 2020.

³ "Data protection - GOV.UK." <https://www.gov.uk/data-protection>. Accessed 10 Sep. 2020.

⁴ "Art. 4 GDPR – Definitions | General Data Protection" <https://gdpr-info.eu/art-4-gdpr/>. Accessed 10 Sep. 2020.

⁵ "Special Categories of Personal Data - GDPR EU." <https://www.gdpreu.org/the-regulation/key-concepts/special-categories-personal-data/>. Accessed 10 Sep. 2020.

GDPR engagement

The risk exposure has been classified as low. This was determined following an Impact Risk Assessment that was conducted in line with guidance provided by Article 29 of the Data Protection Working Party⁶. There were some considerations in reaching this conclusion, which are documented with justification in the report to the GB. It is important to consider the seven key principles of the GDPR in terms of the breach.

Lawfulness, fairness and transparency

The PII data affected by the breach, had been lawfully held prior to the incident occurring. There is a legitimate business requirement to hold data about staff members, for the purposes of administration (e.g. payroll, training and performance monitoring).

The data was held centrally on an operational system, and had been accessed by a staff member who, importantly, had valid reasons to access the information (e.g. to contact a member of their team who had not turned up to work unexpectedly).

Staff members would have been informed about --- and have agreed to --- the collection and use of this data in line with company policy, and thus be in accordance with the principles of fairness and transparency.

Collected for specified, explicit & legitimate purposes

The data had been collected for specific, legitimate business purposes: it is essential for the payroll department to have records of employee names and addresses for the processing of employee wages and disclosure of salary information to HMRC; the human resources department may post contracts to the staff members' home addresses; the departmental manager may need to access an employee address if that staff member has an accident at work, and so forth.

The staff member would have been informed prior to the collection of their data about the specific purposes the data would be collected, used and stored for, and would have to have given their free consent through their acceptance of the company's data protection policy. However, although the consent of the staff member is sought by the organisation, it is not necessary for the lawful processing of their data⁷, as the data is held on a legitimate basis, and not a consensual one.

⁶ "Article 29 Working Party | European Data Protection Board."
https://edpb.europa.eu/our-work-tools/article-29-working-party_en. Accessed 10 Sep. 2020.

⁷ "What is the 'legitimate interests' basis? | ICO."
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>. Accessed 10 Sep. 2020.

Data minimisation

The data list that was accessed contained only names and addresses. It would not be possible to reduce the data held without affecting the ability of the organisation to pursue their legitimate business interests and fulfil their legal and contractual obligations.

Accuracy & where necessary kept up to date

There is no evidence that the data held was inaccurate or outdated.

Storage limitation

The data that was breached included current employees, and was legitimately stored. There is no suggestion that any ex-employees of the organisation were included in the data breach. However, further investigation revealed that the manager held special category data on their desktop. There will need to be further investigation to determine if the special category data was retained beyond its retention period. If the papers were for members of staff who had left the organisation, the severity of the incident would increase.

In line with this principle, it would be worth exploring whether the manager was the only person capable of accessing the device and if the device was capable of moving premises.

Integrity and confidentiality

In relation to the breach, the integrity of how the data was handled has to be scrutinised as it was taken from the centralised system and processed incorrectly. However, it is also important to consider that this was an isolated incident, which could have been avoided if better local procedures were enforced.

There is no reason to believe that the data may have been compromised while on the managers machine. Online security controls are rigorously enforced within NWIS and have been bolstered by the inception of a new Cyber Security team. NWIS are also certified with ISO 27001, an international standard for information security management. There is some concern however, over how easily the data could have been accessed by other members of the team via means such as remote connection or by viewing the information over the manager's shoulder/ while they are away from the desk. It will be worth exploring if there is a local procedure in place to ensure desktops are locked while left unattended.

Accountability

There are no concerns in regards to accountability as NWIS operate robust data controls in line with the GDPR. There is no cause for concern as compliance is regularly demonstrated from the top down. Examples of this include: the appointment of a data protection officer, the documentation of data processing activities and regular DPIAs (Data protection Impact Assessment).

NWIS Policies in relation to the breach

The All Wales NHS Information Governance Policy stipulates the correct procedures for compliance with data standard legislation within NWIS. In the event of this breach, it is clear that not all the standards were upheld. Section 5.2.1 of the NWIS IG policy dictates the requirement for a Senior Information Risk Officer (SIRO). The SIRO can be used as a point of internal escalation before raising risks with the ICO and, in this instance, will champion the recommendations resulting from the incidents risk assessment.

NWIS policy dictates that all PC devices must be encrypted: this mitigates the risk if an asset with confidential data is lost. This is especially the case for the documents that were stored locally, as if there was no encryption on the manager's device the risk rating would increase significantly, particularly given that the data contained within the documents would have been graded as special category by the ICO.

The NWIS Information Governance policy, section 9 stipulates the "right to monitor work processes to ensure the effectiveness of the service". In the case of this incident, introducing additional or targeted monitoring will not be required. Because it is an isolated incident that had a minimal impact, no disciplinary action has been taken and no suspicious circumstances have been identified.

There is online training via the NHS portal "ESR", the training is mandatory but compliance is driven by local team managers. While an isolated breach may not call for drastic measures, it is possible that further mitigation could be realised with the rollout of additional resources or re-fresher courses.

NHS Wales All Email Policy stipulates that the transfer of personal data between wales.nhs.uk emails are secure. It is worth noting that NWIS operate a mail marshal for filtering and blocking emails suspected to be carrying personal identifiable information, however, it is clear that on this occasion the filter was bypassed. Further investigation will be required to determine why this happened. It is also important to consider that the member of the public would have an email hosted outside of the NWIS domain, this presents further questions as there is potential for the mail to be intercepted by individuals with nefarious intentions (black hat hackers).

NWIS is 'signed up' to "The Wales Accord for the Sharing of Personal Information" (WASPI) framework⁸. The framework sets out information sharing protocols for instances where personal data is regularly shared. Given this, it is important that all instances of PII sharing are applied using the WASPI model. In the event of this breach – there is no indication that the operational system was not set up using the ACCORD protocols; however, they may be value in revisiting it with the view of refinement, especially if the ISP (Internet Sharing Protocols) templates have been updated.

⁸ "Wales Accord on the Sharing of Personal Information - WASPI." <http://www.waspi.org/>. Accessed 10 Sep. 2020.

Actions (compliant with policy) to contain a future data breach of this kind

The manager reported that working with files on a local drive was more efficient than working on the data within the operational system. There is value in exploring this claim in more detail, as if the operational system is too slow, it may not be fit for purpose, thereby encouraging other members of staff to do the same (extracting the data to work on it locally). With this consideration, it may be worth pursuing feedback from other managers within the organisation to get a broader consensus. There may be a systems performance issue or the system may need upgrading. In either case, if the system is found to be causing a bottleneck to the managers workload (to the extent that risks are being taken, as per this example), a system upgrade would be an obvious solution to help mitigate the risk.

While it is not the aim to restrict users, particularly those with elevated responsibilities, there will be an investigation into understanding the benefits of the data being extractable. Use cases will be considered with the provision of removing the functionality if justifiable. If the removal of access is not an option, there would need to be a new procedure introduced to dictate the circumstances under which data can be retrievable which emphasises the seven principles of the GDPR.

The manager in question will be reminded about their responsibilities to ensure that they are adhering to the guidelines set out by the GDPR. This will be done via a formal discussion with the manager, with a reminder to the rest of the team cascaded out via a communal area poster or e-poster.

Section 5.1.7 of the Information Governance policy stipulates that all new projects or data flows must comply with Information Governance practices from the outset. Given this, there would be some value in identifying if the project was subject to a Data Protection Impact Assessment (DPIA) during its inception. A retrospective evaluation may also help to identify other areas of risk that have yet to transpire.

This scenario has presented a larger question for the organisation as a whole: does the manager need this much control over staffing issues? In the first instance with the personal data where the breach occurred, it is somewhat understandable — the manager may want to monitor leave or sickness. There is less of a case, however, for the manager to have access to copies of special category data stored locally on their drive. Given these considerations, it will be worth exploring the option of moving some or all of these functions over to the Human Resources department. HR professionals are more likely to be conscientious of the legal implications of major data breaches. It will also allow for a more centralised system, allowing for easier rollout of new procedures and more consistency in how the data is controlled. The breach occurred as the result of the manager wanting to work “more efficiently”, if the current operational system is time consuming, then moving some or all of the administration duties away from the operational managers is likely to help mitigate risk.

While NWIS already operates under the robust “All Wales Governance Policy” and is fully compliant with the Information Governance toolkit, it will be worth exploring the possibility

of introducing additional procedures at a local level. Any procedure will need to maintain the integrity of the GDPR and would consist of measures or specific conditions, under which the data can be extracted.

Mitigation is already in place by NWIS. Section 5.3 of the All Wales Information Security Policy stipulates that all portable and removable media devices must be encrypted. This would offer some assurance if the special category data was moved onto a portable device.

Actions to be taken in respect of those whose information has been leaked

It is highly unlikely that there would be any detriment or risk of harm to the data subject, particularly as there was no special category data involved in the leak. Given this information, there is no legal requirement to inform the affected data subject or the ICO. This may change if new information comes to light, at which point the risk will need to be reassessed (for example, if the data was released to numerous members of the public, the risk will be more severe).

Report FAO: The Executive Board

Summary

The intention of this report is to inform the executive board of an incident that resulted in a personal data breach from within the operational department at NWIS. The breach occurred after a manager extracted personal data (names and addresses) from an operational system. The manager had full access rights to do this. The data was inadvertently attached to an email and sent to a member of the public.

Further investigation identified special category data stored on the manager's desktop in the form of sick notes and occupational health reports. The manager's device is encrypted in line with the NWIS Information Security Policy. There is no evidence that this data was breached.

Data protection implications

The ICO defines a personal data breach as follows:

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

In the case of this breach, it is clear that confidentiality of personal data was lost as the result of an accident.

The Integrity and Confidentiality principles of the GDPR have been brought into dispute as there can be an argument made that the manager was not storing the data correctly in line with best practices. Moreover, special category data was stored on the managers device as opposed to a centralised system: this raises questions of confidentiality which will need to be investigated further.

While the data was being lawfully held, there are questions around the fairness and transparency of how it is being used. It is hoped that stricter local procedures on data control will help to rectify this.

Risk exposure

An Impact Risk Assessment was conducted in line with Article 29 of the Data Protection Working Party⁹ and the incident was classified as low risk.

The Centre for Information Policy Leadership (CIPL) Risk Matrix¹⁰ was evaluated and deemed an appropriate, thorough framework for the risk assessment. The possible harms and threats that could result from a data breach were assessed to determine the likelihood and severity of consequences to the individuals affected by the breach.

The breach involved the data of living persons, but was unlikely to cause physical, material or immaterial harm to any of those affected. Their rights and freedoms were unlikely to be affected by the release of their names and addresses to a single individual. There could feasibly be a small increased risk of identity fraud or similar, and as such the risk matrix score was determined to be approximately 10/300. The assessment determined that the data breach was an isolated incident with low impact in conjunction with the principles discussed in the previous section.

Internal investigation and resultant remedial actions will be sufficient in this case, but records will be kept in case further information comes to light that would necessitate a report to the ICO. It would be necessary to provide this rationale in order to justify not reporting the incident to the ICO within the required 72 hours.

The improperly stored special category data discovered during investigation has been identified as a risk to the organisation, but there has been no unauthorised disclosure of this data. The risks for the special category data were identified using the CIPL risk matrix.

It was determined that there was a moderate risk and likelihood of embarrassment or anxiety; discrimination (for example, it is feasible that disability status or sexual orientation of an individual could be disclosed in a fit note where it was relevant to their health); and a very small, unlikely risk of bodily harm in the event this data was inadvertently disclosed. These harms would come about from inappropriate use or security breach of the data. The risk matrix score was 105/300. The previous breach by the manager who stored the data suggests that the likelihood of a breach of this kind is higher than initially assessed by the organisation and should be dealt with proactively.

The consequences of a breach of special category data would be much more severe, and therefore action is necessary to protect the organisation and the data it is entrusted with from future risk.

⁹ "Article 29 Working Party | European Data Protection Board."

https://edpb.europa.eu/our-work-tools/article-29-working-party_en. Accessed 10 Sep. 2020.

¹⁰ "Risk, High Risk, Risk Assessments and Data Protection Impact" 21 Dec. 2016, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf. Accessed 10 Sep. 2020.

Action required

- Perform thorough review of the operational system:
 - Obtain feedback from managers
 - “Is the operational system fit for purpose?”
 - “Would you be able to perform your work without the ability to extract data from the operational system?”
 - Investigate possibility of performance issues
 - Upgrade the system if appropriate
 - Pursue further refinements or updates in line with ACCORD principles
 - Discuss the benefits of the data being extractable
 - Remove functionality if appropriate
 - Alternately, introduce a procedure to dictate the circumstances under which data can be retrievable from the system
 - Repeat Data Protection Impact Assessment to identify and mitigate risks that are as yet unidentified
- Formal discussion with the manager involved about their data protection responsibilities under the GDPR
- Communal poster or e-poster to remind all staff about their responsibilities under the GDPR
- Investigation to determine reason the NWIS mail marshal did not filter the email
- Consider moving control of special category data, and all administration and staffing issues relating to it, to Human Resources to mitigate risk.

There is no requirement to report the breach to the data subjects or the ICO.

The rationale for these actions and more detailed discussion can be found in a report sent to the Head of Information Governance, copies of which can be obtained on request.

Other considerations

It is clear that given the circumstances involved in the breach, it could have been much more serious. For example, consider a scenario where the names and addresses were not attached, but rather the sick notes and occupational health reports. The ramifications of this breach would carry much higher consequences given the category of data, particularly as there is likely to be emotional distress for the staff members whose details have leaked. It is important to consider this when determining the correct action when referring to the ICO.

The Article 29 Working Party defines risk, as *"This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached"*. In this case, the impact on the data subject would be more severe and the Incident would be referred to the ICO.

Report FAO: Information Governance Committee

Summary

The purpose of this report is to outline an isolated incident that resulted in a breach of confidential personal data from within the operational department to a single member of the public.

The data breach consisted of a file containing the personally identifiable information (comprised of names and addresses) of staff members; no special category data was involved. The data was downloaded from a central operational system onto an encrypted local device. The file was accessed by the operational manager, who had the appropriate privileges and valid reasons to do so. The file was downloaded onto the local device by the manager with the intention of "*working more efficiently*", and then inadvertently emailed to a single individual outside of the organisation, in what was a clear breach of the Data Protection Act 2018.

Investigation revealed further cause for concern, as special category data (scanned copies of fit notes and occupational health reports) was discovered on the manager's device: this data was not involved in the data breach.

GDPR breach

The data was lawfully held on a legitimate basis prior to the incident. There is a legitimate business requirement to hold the data involved and a staff member with a valid business reason to do so accessed it. The data related to current staff members only, and was sent to a single, external recipient. The data was minimal, containing only names and addresses: no special category data was sent. There is no evidence that the data was in any way inaccurate. The data breach was not caused by a system or device security flaw. The organisation's data compliance policies or their enforcement were not contributory factors in the data breach.

The specific principle of the GDPR that was contravened in the incident was that of "*Integrity and Confidentiality*": the data was removed from the centralised system and then processed incorrectly by the manager.

Further contraventions of GDPR principles were discovered during investigation of the incident: the storage of special category data by the manager on a local device. Special category data stored outside of an approved NWIS system (even on an encrypted device) does not satisfy the GDPR principles of "*Storage limitation*": it is not known whether the data has been retained beyond its retention period or relates to ex-employees, as it has escaped the organisations' purview to date.

Risk exposure

An Impact Risk Assessment was conducted in line with Article 29 of the Data Protection Working Party and the incident was classified as low risk. The data breach was an isolated incident with low impact in conjunction with the principles discussed in the previous section.

The improperly stored special category data discovered during investigation has been identified as a risk to the organisation, but there has been no unauthorised disclosure of this data. The consequences of a breach of special category data would be much more severe.

Action required

The organisation should consider whether a procedural change is necessary in order to remove the requirement for managers to process special category data. The future control of special category data could fall under the remit of the Human Resources Department to mitigate risk and ensure GDPR compliance.

An in depth review of the operational system that stored the data involved in the breach will be undertaken, to determine whether performance improvements or modifications to functionality would prevent similar breaches in the future.

A formal discussion will be held with the employee who caused the data to be disclosed. Employees of the organisation will be reminded of their responsibilities under the GDPR via email, and posters displayed in common areas.

There is no requirement to report the breach to the data subjects or the ICO.

The rationale for these actions and more detailed discussion can be found in a report sent to the Head of Information Governance, copies of which can be obtained on request.

NWIS data protection policies

All NWIS Policies referenced in this document can be found at the following link:

<http://www.wales.nhs.uk/sites3/Documents/950/>